

PATENT ABSTRACTS OF JAPAN

(11)Publication number : 2004-107959

(43)Date of publication of application : 08.04.2004

(51)Int.Cl.

E05B 49/00
B60R 25/00
H04Q 9/00

(21)Application number : 2002-270543

(71)Applicant : DENSO CORP

(22)Date of filing : 17.09.2002

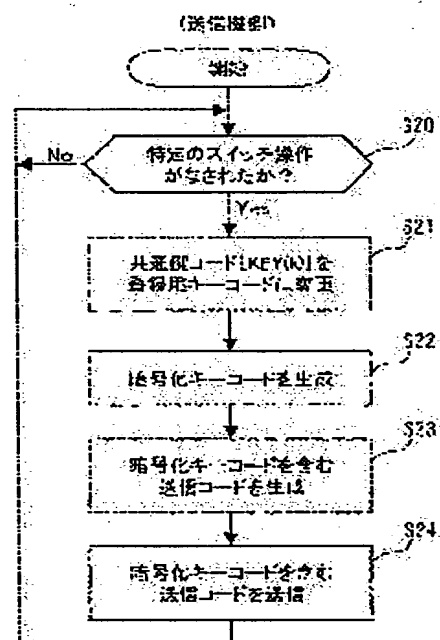
(72)Inventor : TSUJI HIROYUKI
OKUMURA RYOZO

(54) REMOTE CONTROLLER

(57)Abstract:

PROBLEM TO BE SOLVED: To prevent a key code from being decoded when the key code is transmitted from a transmitter to a receiver for registration.

SOLUTION: In a transmitter, when a specified switch is operated, the k-th of a common key code used for a translate table to encipher a key code is changed (step S21) to a key code for registration stored in advance, and the key code is enciphered by use of the transrate table containing the key code for registration (step S22). A transmission code with an attached specified code is made (step S23) and the signal for the transmission code is transmitted to a receiver (step S24). Thereby, even if a transmission signal is eavesdropped when a transmission code is transmitted from the transmitter to the receiver, since the key code is enciphered and transmitted, the key code can not easily decoded.



LEGAL STATUS

[Date of request for examination] 17.01.2005

[Date of sending the examiner's decision of rejection]

[Kind of final disposal of application other than the examiner's decision of rejection or application converted registration]

[Date of final disposal for application]

[Patent number]

[Date of registration]

[Number of appeal against examiner's decision of rejection]

[Date of requesting appeal against examiner's decision of rejection]

[Date of extinction of right]

(19) 日本国特許庁(JP)

(12) 公開特許公報(A)

(11) 特許出願公開番号

特開2004-107959

(P2004-107959A)

(43) 公開日 平成16年4月8日(2004.4.8)

(51) Int.Cl. ⁷	F I	テーマコード (参考)
E 05 B 49/00	E 05 B 49/00 K	2 E 2 5 0
B 6 0 R 25/00	B 6 0 R 25/00 6 0 6	5 K 0 4 8
H 0 4 Q 9/00	H 0 4 Q 9/00 3 0 1 B	

審査請求 未請求 請求項の数 4 O L (全 18 頁)

(21) 出願番号	特願2002-270543 (P2002-270543)	(71) 出願人	000004260
(22) 出願日	平成14年9月17日 (2002.9.17)		株式会社デンソー
			愛知県刈谷市昭和町1丁目1番地
		(74) 代理人	100106149
			弁理士 矢作 和行
		(72) 発明者	辻 浩幸
			愛知県刈谷市昭和町1丁目1番地 株式会
			社デンソー内
		(72) 発明者	奥村 亮三
			愛知県刈谷市昭和町1丁目1番地 株式会
			社デンソー内
		F ターム (参考)	2E250 AA21 BB08 DD06 EE02 EE08
			EE10 EE14 FF24 FF36 GG08
			GG15 HH01 JJ03 KK03 LL01
			LL14 LL20 TT03

最終頁に続く

(54) 【発明の名称】 遠隔操作装置

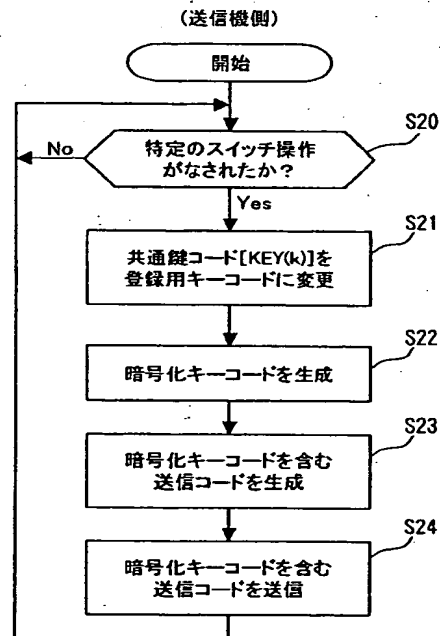
(57) 【要約】

【課題】 送信機から受信機へキーコードを送信して登録するときのキーコードの解読を防止する。

【解決手段】 送信機において、特定のスイッチ操作がなされた場合に、キーコードを暗号化する変換テーブルに用いる共通鍵コードのk番目を、予め記憶している登録用キーコードに変更し（ステップS21）、この登録用キーコードを含む変換テーブルを用いてキーコードを暗号する（ステップS22）。そして、暗号化されたキーコードに、所定のコードを付して送信コードを生成し（ステップS23）、この送信コードの信号を受信機へ送信する（ステップS24）。これにより、送信機から受信機に送信コードを送信しているときに、例えば送信コードが盗聴されたとしても、キーコードは暗号化されて送信しているため、キーコードが容易に解読されることがなくなる。

【選択図】

図8



【特許請求の範囲】

【請求項 1】

装置毎に固有に定められた固有キーコードを用いて所定のコードを暗号化する暗号化手段を有し、この暗号化手段によって暗号化された暗号化コードを送信する送信機と、前記暗号化コードを受信し前記固有キーコードを用いて前記暗号化コードを復号化する復号化手段を有し、この復号化手段によって復号化されたコードが記憶されているコードに対して所定の関係を満足しているときに、制御対象を作動させる指令を出力する受信機とを備える遠隔操作装置であって、前記復号化手段が用いる前記固有キーコードを前記送信機から前記受信機へ送信して登録する場合、前記送信機は前記送信機及び前記受信機が記憶するデフォルトキーコードを用いて前記暗号化手段によって前記固有キーコードを暗号化したうえで前記受信機に対して送信することを特徴とする遠隔操作装置。

10

【請求項 2】

前記送信機は、所定の操作がなされた場合に前記暗号化した固有キーコードを前記受信機に対して送信することを特徴とする請求項 1 記載の遠隔操作装置。

【請求項 3】

装置毎に固有に定められた固有キーコードを用いて受信した所定のコードを暗号化する暗号化手段を有し、この暗号化手段によって暗号化された暗号化コードを送信する携帯機と

前記携帯機に対して前記所定のコードを送信するとともに、その所定のコードに対して返送された前記暗号化コードを受信し前記固有キーコードを用いて前記暗号化コードを復号化する復号化手段を有し、この復号化手段によって復号化されたコードが送信したコードに対して所定の関係を満足しているときに、制御対象を作動させる指令を出力する車載制御機とを備える遠隔操作装置であって、

20

前記復号化手段が用いる前記固有キーコードを前記携帯機から前記車載制御機へ送信して登録する場合、前記携帯機は前記携帯機及び前記車載制御機が記憶するデフォルトキーコードを用いて前記暗号化手段によって前記固有キーコードを暗号化したうえで前記車載制御機に対して送信することを特徴とする遠隔操作装置。

【請求項 4】

前記携帯機は、所定の操作がなされた場合に前記暗号化した固有キーコードを前記車載制御機に対して送信することを特徴とする請求項 3 記載の遠隔操作装置。

30

【発明の詳細な説明】

【0001】

【発明の属する技術分野】

本発明は、車両のワイヤレスドアロック制御等に用いられる遠隔操作装置に関するものである。

【0002】

【従来の技術】

従来、車両のワイヤレスドアロック制御等に用いられる遠隔操作装置では、盗聴などの不正防止の観点から、送信機から送信する送信コードを暗号化して、ユーザによって解読されないように対策している。例えば、特許文献 1 に開示されている遠隔操作装置では、送信機が送信する毎に所定の順序で変更されるローリングコードを、装置毎に固有に定めたキーコードを用いて暗号化して暗号化ローリングコードを生成し、この暗号化ローリングコードを用いて ID コードをさらに暗号化している。そして、これらのコードを受信する受信機では、暗号化された暗号化ローリングコード及び ID コードを復元し、復元した ID コードが記憶している ID コードに一致し、かつ、復元したローリングコードと記憶されるローリングコードとが所定の関係を満足している場合に、制御対象への指示信号を出力している。

40

【0003】

このように、従来の遠隔操作装置では、ローリングコードを単に送信して照合するのでは

50

なく、キーコードという送信機と受信機とが共通して記憶するコードを用いてローリングコードを暗号化している。

【0004】

【特許文献1】

特開平10-61277号公報

【0005】

【発明が解決しようとする課題】

上述のローリングコードの暗号化に用いられるキーコードは、遠隔操作装置を製造する工程において、送信機から受信機に対してキーコードを送信し、受信機の不揮発性記憶媒体に記憶する。しかし、この従来の遠隔操作装置では、送信機から受信機へキーコードを送信する際、このキーコードを暗号化しない状態で送信機から送信していたため、この送信時にキーコードが盗聴される恐れがあった。そのため、キーコードによって暗号化されるローリングコードは、予め設定された順序で変更されるものであるため、例えば、この変更順序を設定した者（設計者）がキーコードを取得したならば、暗号化されたローリングコード及びIDコードの解読が可能となる。

【0006】

本発明は、かかる問題を鑑みてなされたもので、受信機へキーコードを登録するときのキーコードの取得を防止することが可能な遠隔操作装置を提供することを目的とする。

【0007】

【課題を解決するための手段】

請求項1に記載の遠隔操作装置は、装置毎に固有に定められた固有キーコードを用いて所定のコードを暗号化する暗号化手段を有し、この暗号化手段によって暗号化された暗号化コードを送信する送信機と、暗号化コードを受信し固有キーコードを用いて暗号化コードを復号化する復号化手段を有し、この復号化手段によって復号化されたコードが所定の関係を満足しているときに、制御対象を作動させる指令を出力する受信機とを備える遠隔操作装置であって、復号化手段が用いる固有キーコードを送信機から受信機へ送信して登録する場合、送信機は送信機及び受信機が記憶する所定の共通キーコードを用いて暗号化手段によって固有キーコードを暗号化したうえで受信機に対して送信することを特徴とする。

【0008】

このように、例えば、車両のワイヤレスドアロック制御等に用いられる本発明の遠隔操作装置は、送信機の固有キーコードを暗号化したうえで受信機へ送信している。これにより、送信機の固有キーコードを受信機へ送信して登録する際、固有キーコードが盗聴されたとしても、固有キーコードは暗号化されているため、固有キーコードの取得の困難性が向上できる。その結果、送信機の不正な複製を防止することが可能となる。

【0009】

また、固有キーコードの暗号化は、制御対象を作動させるための所定のコードを暗号化する暗号化手段によって暗号化されるため、専用の暗号化アルゴリズムを用意する必要がなく、ソフト容量の節約や管理工数が削減できる。

【0010】

請求項2に記載の遠隔操作装置によれば、送信機は、所定の操作がなされた場合に暗号化した固有キーコードを受信機に対して送信することを特徴とする。例えば、ユーザが通常することのない押しボタンの押し方、押す順序等を固有キーコードの登録に割り当ておくことで、固有キーコードを容易に受信機へ送信することが可能となる。

【0011】

請求項3に記載の遠隔操作装置は、装置毎に固有に定められた固有キーコードを用いて受信した所定のコードを暗号化する暗号化手段を有し、この暗号化手段によって暗号化された暗号化コードを送信する携帯機と、携帯機に対して所定のコードを送信するとともに、その所定のコードに対して返送された暗号化コードを受信し固有キーコードを用いて暗号化コードを復号化する復号化手段を有し、この復号化手段によって復号化されたコードが

所定の関係を満足しているときに、制御対象を作動させる指令を出力する車載制御機とを備える遠隔操作装置であって、復号化手段が用いる固有キーコードを携帯機から車載制御機へ送信して登録する場合、携帯機は携帯機及び車載制御機が記憶する所定の共通キーコードを用いて暗号化手段によって固有キーコードを暗号化したうえで車載制御機に対して送信することを特徴とする。

【0012】

このように、携帯機と車載制御機との双方向通信によって、例えば、車両の各ドアのロック機構やステアリングロック機構を制御したり、車両のエンジンの始動の許可・禁止状態を制御したりする電子キーシステムに、本発明の遠隔操作装置を適用することによって、固有キーコードの取得を困難なものとすることができる。その結果、携帯機の不正な複製を防止することが可能となる。

【0013】

請求項4に記載の遠隔操作装置によれば、携帯機は、所定の操作がなされた場合に暗号化した固有キーコードを車載制御機に対して送信することを特徴とする。例えば、ユーザが通常することのない押しボタンの押し方、押す順序等を固有キーコードの登録に割り当てておくことで、固有キーコードを容易に受信機へ送信することが可能となる。

【0014】

【発明の実施の形態】

以下、本発明の実施の形態における遠隔操作装置に関して、図面に基づいて説明する。

【0015】

(第1の実施形態)

本実施形態では、本発明の遠隔操作装置を車両用のワイヤレスドアロック制御等を行う装置に採用した例について説明する。図1は、本実施形態の遠隔操作装置における、送信機1と受信機2の構成を示すブロック図である。

【0016】

同図において、送信機1には、それぞれ異なった機能(例えば、車両の各ドアのロック・アンロック、トランクの開閉、シートポジションの設定等)を遠隔作動させるためのスイッチ12-1、12-2、・・・、12-nが設けられており、そのスイッチ操作による信号がマイクロプロセッサ11に入力するように構成されている。

【0017】

このマイクロプロセッサ11は、EEPROM13が接続されており、このEEPROM13には、送信機固有のIDコード、送信機1が送信する毎に所定の順序で変化するローリングコード、車両固有のキーコード、及び登録用キーコード(デフォルトキーコード)が記憶されている。これらのIDコード、ローリングコード、キーコード、登録用キーコードは、車両の製造工程においてEEPROM13に記憶されるものである。

【0018】

また、EEPROM13には、マイクロプロセッサ11がローリングコードを暗号化する際に用いる変更テーブル(図2)が記憶されるとともに、暗号化アルゴリズム(図3)がプログラムとして記憶されている。このプログラムに従って、マイクロプロセッサ11にて暗号化処理が行われる。

【0019】

図2に示すように、変更テーブルは、各々異なるmビットからなるn個の共通鍵コード[KEY(1)~KEY(n)]が設定されている。このうち、k番目の共通鍵コードには、EEPROM13に記憶される車両固有のキーコードが設定されている。

【0020】

さらに、マイクロプロセッサ11には、発信回路14及びFM変調回路15が接続されており、マイクロプロセッサ11にて最終的に生成された送信コードを、FM変調したのち微弱電波として発信するように構成されている。

【0021】

受信機2は、送信機1から発信された微弱電波を復調する受信回路が設けられている。こ

10

20

30

40

50

の受信回路は、局部発振器 24、高周波増幅回路 25、ミキサ回路 26、中間周波増幅回路 27、復調回路 28 によって構成され、その復調された出力信号がマイクロプロセッサ 21 に入力されるように構成されている。なお、このマイクロプロセッサ 21 は、予め定められた処理に基づいて、復調された出力信号から暗号化されたローリングコードを復元する。

【0022】

マイクロプロセッサ 21 には、EEPROM 29 が接続されており、この EEPROM 29 には、受信機 2 固有の ID コード、送信機 1 から前回受信した送信コードに含まれていたローリングコード、車両固有のキーコード、及び登録用キーコードが記憶されている。なお、この ID コード、車両固有のキーコード、及び登録用キーコードの各コードは、送信機が記憶する ID コード、車両固有のキーコード、及び登録用キーコードの各々と同一の内容となっている。

【0023】

また、EEPROM 29 には、マイクロプロセッサ 21 が暗号化されたローリングコードを復元する際に用いる変更テーブル（図 2 と同じ）が記憶されるとともに、出力信号から暗号化ローリングコードを復元するための復号化アルゴリズムがプログラムとして記憶されている。

【0024】

さらに、マイクロプロセッサ 21 には、駆動回路 23-1、23-2、・・・、23-n を介して、制御対象となる 22-1、22-2、・・・、22-n（例えば、車両の各ドアのロック・アンロック、トランクの開閉、シートポジションの設定等を行うアクチュエータ）が接続されており、この制御対象となる 22-1、22-2、・・・、22-n は、マイクロプロセッサ 21 からの信号に応じて作動するように構成されている。

【0025】

（通常動作）

次に、上記構成の送信機 1 及び受信機 2 による、制御対象を遠隔操作する際の動作について、図 4 及び図 5 のフローチャートを用いて説明する。まず、図 4 のステップ S1 では、送信機 1 のスイッチ 12-1、12-2、・・・、12-n のいずれかが操作されたか否かを判断する。ここで、いずれかのスイッチが操作された場合には、ステップ S2 へ処理を進め、いずれのスイッチも操作されていない場合には、操作されるまで待機状態となる。

【0026】

ステップ S2 では、EEPROM 13 に記憶されるローリングコードの更新を行う。このローリングコードは、m ビットからなる変数で、送信機 1 から送信が行われる毎に、所定の規則（例えば、シフト演算等）に従って変化する。

【0027】

ステップ S3 では、ローリングコードを暗号化して暗号化ローリングコードを生成する。この暗号化ローリングコードの生成方法を、図 2 に示す変換テーブル及び図 3 に示す暗号化アルゴリズムを用いて説明する。

【0028】

まず、図 3 において、図 2 に示す 1 番目の共通鍵コード [KEY (1)] とローリングコードとの排他的論理和の演算を行う。次に、排他的論理和の演算結果に対して、周知の M 系列演算を行う。その後、2 番目以降の共通鍵コードを用いた排他的論理和の演算と M 系列演算を (n-1) 回繰り返す。これにより、ローリングコードが暗号化され、最終的に暗号化ローリングコードが生成される。

【0029】

なお、k 回目の排他的論理和の演算では、車両固有のキーコードが k 番目の共通鍵コード [KEY (k)] として用いている。これにより、k 回目の排他的論理和の演算方法は車両毎に異なることになり、さらには、暗号化の方法が車両によって異なることになる。

【0030】

10

20

30

40

50

ステップS 4では、ステップS 3において暗号化された暗号化ローリングコード、EEPROM 13に記憶されるIDコード、及び機能コードを用いて送信コードを生成する。この送信コードは、例えば、これらの各コードにフォーマットビット（スタートビット、ストップビット、パリティビット）を付加し、さらに所定ビット数からなる乱数を加えて送信コードを構成する。

【0031】

なお、機能コードとは、制御対象となる22-1、22-2、・・・、22-nを作動させるためのコードであり、ステップS 1において操作された各機能（例えば、車両の各ドアのロック・アンロック、トランクの開閉、シートポジションの設定等）を遠隔作動させるためのスイッチ12-1、12-2、・・・、12-nに対応したものである。

10

【0032】

そして、ステップS 5において、ステップS 4で生成した送信コードをFM変調回路15を介して出力する。これにより、送信コードはFM変調されて微弱電波として送信機1の外部に発信される。

【0033】

続いて、受信機2が上述の送信コードを受信してから制御対象に制御指令を出力するまでの動作について、図5のフローチャートを用いて説明する。まず、ステップS 10において、送信機1からの送信コードを受信したか否かを判断する。ここで、送信コードを受信した場合には、ステップS 11へ処理を進め、送信コードを受信していない場合には、受信するまで待機状態となる。

20

【0034】

ステップS 11では、送信コードから暗号化ローリングコード、IDコード及び機能コードを抽出し、この抽出した暗号化ローリングコードを復元する。なお、暗号化ローリングコードの復元には復号化アルゴリズムが用いられる。そして、ステップS 12において、抽出したIDコードとEEPROM 29に記憶されているIDコードとが一致するか否かを判断する。ここで、IDコードが一致するならば、ステップS 13へ処理を進め、これに該当しない場合には、ステップS 10へ処理を移行し、再び送信コードの受信待ちとなる。

【0035】

ステップS 13では、ステップS 11において復元されたローリングコードと、EEPROM 29に記憶されているローリングコードとを比較し、復元されたローリングコードが記憶されるローリングコードに対し、所定の範囲内にあるか否かを判定する。ここで、所定の範囲内にある場合には、ステップS 14へ処理を進め、これに該当しない場合には、ステップS 10へ処理を移行し、再び送信コードの受信待ちとなる。

30

【0036】

なお、ステップS 13では、送信機1から送信される送信コードが、受信機2で毎回確実に受信できない場合を考慮している。すなわち、送信機1から送信コードが送信されても、例えば電波干渉等の理由により、受信機2で送信コードが受信できない（いわゆる送信機1のカラ打ち）場合がある。このとき、送信機1のローリングコードのみが更新されるため、このカラ打ちに対応できるように、許容範囲を定めている。

40

【0037】

このように、本実施形態では、復号化されたローリングコードが、予め定められた関係を満足しているか否かを判定している。

【0038】

ステップS 14では、受信機2のEEPROM 29に記憶されているローリングコードを一旦消去したのち、送信コードから復元したローリングコードを新たなローリングコードとして記憶する。以後、ステップS 13の処理では、この新たに記憶されたローリングコードと復元したローリングコードとを比較する。そして、ステップS 15において、送信コードに設定されていた機能コードを参照し、駆動回路23-1、23-2、・・・、23-nを介して、制御対象となる22-1、22-2、・・・、22-nを作動させる。

50

【0039】

(キーコード登録)

次に、本実施形態の特徴部分である、車両固有のキーコードを送信機1から受信機2へ送信して登録する際の、送信機1及び受信機2の動作について、図8及び図9のフローチャートを用いて説明する。なお、送信機1から登録すべきキーコードを送信する前に、受信機2をキーコード登録のモードに予め変更しておく。このモード変更については、例えば、別途用意される登録専用の送信機等からモード変更の信号を受信機2に対して送信するなどして、モードを変更する。

【0040】

さらに、受信機2のモードがキーコード登録モードに変更されたとき、キーコードを復号化するための変換テーブル(図2と同じ)のk番目の共通鍵コード[KEY(k)]を、EEPROM29に記憶される登録用のキーコードに変更する。この登録用キーコードは、mビットからなる変数であり、例えば、0000やffff等である。

【0041】

まず、ステップS20は、送信機1におけるスイッチ12-1、12-2、・・・、12-nの特定の操作がなされたか否かを判断する。ここで、特定の操作がなされた場合には、ステップS21へ処理を進め、これに該当しない場合には、スイッチ操作がなされるまで待機状態となる。この特定のスイッチ操作がなされた場合に、送信機1ではキーコードを暗号化して受信機2へ送信する。従って、送信機1の登録すべきキーコードを容易に受信機2へ送信することができる。

【0042】

なお、この特定のスイッチ操作とは、通常、ユーザが制御対象を遠隔操作するために操作するスイッチの押し方とは異なるもので、例えば、特定の複数のスイッチ12-1、12-2、・・・、12-nを同時に押したり、複数のスイッチ12-1、12-2、・・・、12-nを特定の順序で押したりする操作である。但し、キーコードを暗号化して送信させるための操作として、このようなスイッチ操作に限定されるものではない。

【0043】

ステップS21では、図6に示すように、EEPROM13に記憶される変換テーブルのうち、k番目の共通鍵コード[KEY(k)]を、同じくEEPROM13に記憶される登録用キーコードに変更する。この登録用キーコードは、上述の如く、mビットからなる変数であり、例えば、0000やffff等である。

【0044】

ステップS22では、EEPROM13に記憶される車両固有のキーコードを抽出し、これを暗号化して暗号化キーコードを生成する。この暗号化キーコードの生成方法については、上述のローリングコードを暗号化して暗号化ローリングコードを生成する方法と同一であり、図6に示す変換テーブルのk番目の共通鍵コードに登録用キーコードを用いた点と、図7に示すように、暗号化アルゴリズムを用いて暗号化する対象が車両固有のキーコードになる点のみ異なる。よって、暗号化キーコードの生成方法に関する説明は省略する。

【0045】

このように、本実施形態におけるキーコードの暗号化は、制御対象を遠隔操作する際のローリングコードを暗号化する暗号化アルゴリズムを使用するため、専用の暗号化アルゴリズムを用意する必要がなく、ソフト容量の節約や管理工数が削減できる。

【0046】

ステップS23では、ステップS22において暗号化された暗号化キーコード、及びEEPROM13に記憶されるIDコードを用いて送信コードを生成する。この送信コードは、上述のように、例えば、これらの各コードにフォーマットビット(スタートビット、ストップビット、パリティビット)を付加し、さらに所定ビット数からなる乱数を加えて送信コードを構成する。

【0047】

10

20

30

40

50

そして、ステップS 2 4において、ステップS 2 3で生成した送信コードをFM変調回路1 5を介して出力する。これにより、暗号化キーコードを含む送信コードがFM変調されて、微弱電波として送信機1の外部に発信される。

【0048】

続いて、受信機2が上述の暗号化キーコードを含む送信コードを受信し、復元したキーコードを記憶するまでの動作について、図9のフローチャートを用いて説明する。まず、ステップS 3 0において、送信機1からの送信コードを受信したか否かを判断する。ここで、送信コードを受信した場合には、ステップS 3 1へ処理を進め、送信コードを受信していない場合には、受信するまで待機状態となる。

【0049】

ステップS 3 1では、送信コードからIDコード及び暗号化キーコードを抽出し、抽出した暗号化キーコードを復元する。なお、暗号化キーコードの復元は、登録用キーコードが設定された変更テーブルを用いて復元する。そして、ステップS 3 2において、抽出したIDコードとEEPROM29に記憶されているIDコードとが一致するかどうかを判断する。ここで、IDコードが一致するならば、ステップS 3 3へ処理を進め、これに該当しない場合には、ステップS 1 0へ処理を移行し、再び送信コードの受信待ちとなる。

【0050】

ステップS 3 3では、送信コードから復元したキーコードを受信機2のEEPROM29へ記憶する。あるいは、既にキーコードがEEPROM29に記憶されている場合には、既に記憶されているキーコードを一旦消去したのち記憶する。

【0051】

このように、本実施形態の遠隔操作装置は、送信機1のキーコードを暗号化したうえで受信機2へ送信している。これにより、キーコードを送信機1から受信機2へ送信して登録する際、仮に、この送信時に暗号化されたキーコードが盗聴されたとしても、キーコード取得の困難性を向上することができる。その結果、送信機1の不正な複製を防止することが可能となる。

【0052】

なお、本実施形態において説明した暗号化アルゴリズム及び復号化アルゴリズムは、排他的論理和の演算やM系列演算による暗号化に限定されるものではない。

【0053】

また、通常動作及びキーコード登録の処理において、送信機1から送信される送信コードに含まれるIDコードを暗号化しても良い。そして、暗号化されたIDコードを含む送信コードを送信し、この送信コードを受信する受信機2において暗号化されたIDコードを復元しても良い。

【0054】

(第2の実施形態)

本実施形態では、本発明の遠隔操作装置を電子キーシステムに採用した例について説明する。本実施形態の電子キーシステムは、携帯機(電子キー)側と車両側との双方向通信による車両の内外での所定コードの照合結果を基に、車両に設けられたセキュリティECUが各ドアのロック機構やステアリング機構を制御し、さらに、車両のエンジンの始動の許可・禁止状態を制御するものである。

【0055】

図10は、本実施形態の電子キーシステムの全体の構成を示す図である。同図に示すように、車両32には車両側発信機33が設けられ、セキュリティECU35からの指示に基づいて、所定間隔毎にチャレンジコード信号を発信する。この車両側発信機33は、車両32の複数箇所に設けられ、かつ、それぞれの発信機33から発信されるチャレンジコード信号の到達距離が設定されている。従って、このチャレンジコード信号の到達距離に応じた検知エリア31が車両32の周囲に形成され、携帯機30の携帯者が車両32に接近したことを即座に検知できるようにしている。

【0056】

10

20

30

40

50

携帯機 30 は、車両側発信機 33 からのチャレンジコード信号を受信したり、暗号化したチャレンジコードと ID コードとを含む送信コード信号を送信したりする送受信回路（図示せず）を備えている。また、受信したチャレンジコード信号を暗号化するマイクロプロセッサ（図示せず）と、携帯機 30 固有の ID コード、車両固有のキーコード及び登録用キーコード（デフォルトキーコード）を記憶する RAM（図示せず）も備えている。

【0057】

また、この RAM には、チャレンジコードを暗号化する際に用いる変更テーブル（図 11）が記憶されるとともに、暗号化アルゴリズム（図 12）がプログラムとして記憶されている。従って、携帯機 30 が検知エリア 31 内に入ったとき、携帯機 30 は、即座にチャレンジコード信号を受信し、この受信したチャレンジコードを暗号化したのち、ID コードを付した送信コード信号を発信する。

10

【0058】

なお、図 11 に示すように、変更テーブルは、各々異なる m ビットからなる n 個の共通鍵コード [KEY (1) ~ KEY (n)] が設定されている。このうち、k 番目の共通鍵コードには、RAM に記憶されている車両固有のキーコードが設定されている。

【0059】

携帯機 30 から発信された送信コード信号は、車両 32 に設けられたワイヤレスレシーバ 34 によって受信される。この受信した送信コード信号は、セキュリティ ECU 35 に出力され、セキュリティ ECU 35 にて、暗号化されたチャレンジコードが復元される。

【0060】

このセキュリティ ECU 35 は、図示しない RAM を有し、この RAM には、暗号化されたチャレンジコードを復元する際に用いる変更テーブル（図 11 と同じ）が記憶されるとともに、暗号化されたチャレンジコードを復元するための復号化アルゴリズムがプログラムとして記憶されている。さらに、この RAM には、車両固有のキーコード及び登録用キーコードが記憶されている。

20

【0061】

セキュリティ ECU 35 は、ID コード及び暗号化されたチャレンジコードを抽出し、この暗号化されたチャレンジコードを復元する。そして、RAM に記憶されている ID コードと抽出した ID コードとが一致したか否かを判定する。さらに、車両側発信機 33 から発信した RAM に記憶されるチャレンジコードと復元したチャレンジコードとが一致したか否かを判定する。

30

【0062】

ここで、ID コード及びチャレンジコードの両方が一致したと判定されると、ドアロック機構 36 やラゲージドアロック機構 39 をアンロックスタンバイ状態にする。そして、ドアハンドルに設けられたタッチスイッチ（図示しない）によって、ドアハンドルの操作の開始が検出されると、ドアやラゲージドアをアンロック状態にする。

【0063】

このように、本実施形態では、復元されたチャレンジコードが予め定めた関係を満足しているか否かを判定している。

【0064】

一方、ドアを開閉して携帯機 30 の携帯者が乗車すると、車室内に設けられた車両側発信機 33 及びワイヤレスレシーバ 34 を用いて携帯機 30 との間で双方向通信を行い、再度、ID コード及びチャレンジコードの照合を行う。このとき、ID コードの照合結果及びチャレンジコードの照合結果が「一致」であると、ステアリンクロック機構 37 をアンロックスタンバイ状態にする。この状態で、予め車両 32 に設けられているエンジンスイッチ（図示せず）が操作されると、ステアリンクロック機構 37 がアンロックされるとともに、エンジン ECU 38 に対してエンジンの始動禁止を解除するように指示信号を出力する。

40

【0065】

このようにして、携帯機 30 の携帯者は、携帯機 30 を手に取ることなく、ドアのアンロ

50

ックによる乗車からエンジンの始動までを行うことができる。

【0066】

また、車両32が停車し、エンジンスイッチがオフされた後に、携帯機30の携帯者が降車し、ドアハンドルに設けられたドアロックスイッチを操作すると、車両32の各ドアがロックされる。このドアロックと同時に、エンジンECU38によってエンジンが始動禁止状態に設定される。

【0067】

このように、本実施形態における電子キーシステムは、携帯機30を携帯しているのみで、ドアのロック・アンロックを含む車両32のセキュリティの設定・解除を自動的に行うことができるものである。

10

【0068】

(通常動作)

次に、上記構成の携帯機30及び車両32との双方向通信による、ドアロック機構36やラッチゲジロック機構39を遠隔操作する際の動作について、図13及び図14のフローチャートを用いて説明する。

【0069】

まず、図13に示すステップS40では、携帯機30において、車両側発信機33から所定間隔毎に発信されるチャレンジコード信号を受信したか否かを判断する。ここで、チャレンジコード信号を受信した場合には、ステップS41に処理を進め、これに該当しない場合には、チャレンジコード信号を受信するまで待機状態となる。

20

【0070】

ステップS41では、受信したチャレンジコード信号に基づいて、このチャレンジコードを暗号化した暗号化チャレンジコードを生成する。この暗号化チャレンジコードの生成方法を、図11に示す変更テーブル及び図12に示す暗号化アルゴリズムを用いて説明する。

【0071】

まず、図11に示す1番目の共通鍵コード[KEY(1)]と受信したチャレンジコードとの排他的論理和の演算を行う。次に、排他的論理和の演算結果に対して、周知のM系列演算を行う。その後、2番目以降の共通鍵コードを用いて排他的論理和の演算とM系列演算を(n-1)回繰り返す。これにより、チャレンジコードが暗号化され、最終的に暗号化チャレンジコードが生成される。

30

【0072】

なお、k回目の排他的論理和の演算では、車両固有のキーコードが変更テーブルの共通鍵コード[KEY(k)]として用いている。これにより、k回目の排他的論理和の演算方法は、車両毎に異なることになり、さらには、暗号化の方法が車両によって異なることになる。

【0073】

ステップS42では、ステップS41において生成された暗号化チャレンジコード及びRAMに記憶されるIDコードを用いて、送信コードを生成する。この送信コードは、例えば、暗号化チャレンジコード及びIDコードにフォーマットビット(スタートビット、ストップビット、パリティビット)を付加し、さらに所定ビット数からなる乱数を加えて送信コードを構成する。

40

【0074】

そして、ステップS43において、ステップS42において生成した送信コードの信号(送信コード信号)を発信する。

【0075】

次に、図14に示すステップS50では、携帯機30からの送信コード信号を受信したか否かを判断する。ここで、送信コード信号を受信した場合には、ステップS51へ処理を進め、送信コード信号を受信していない場合には、送信コード信号を受信するまで待機状態となる。

50

【0076】

ステップS51では、受信した送信コード信号からIDコード及び暗号化チャレンジコードを抽出し、この抽出した暗号化チャレンジコードを復元する。なお、暗号化チャレンジコードの復号化には、復号化アルゴリズムが用いられる。そして、ステップS52において、抽出したIDコードとセキュリティECU35のRAMに記憶されているIDコードとが一致するか否かを判別する。ここで、IDコードが一致するならば、ステップS53へ処理を進め、IDコードが一致しない場合には、ステップS50へ処理を移行し、再び送信コード信号の受信待ち状態となる。

【0077】

ステップS53では、ステップS51において復元されたチャレンジコードと、車両側発信機33から発信したRAMに記憶されるチャレンジコードとが一致するか否かを判別する。そして、チャレンジコードが一致するならば、ステップS54へ処理を進め、チャレンジコードが一致しない場合には、ステップS50へ処理を移行し、再び送信コード信号の受信待ち状態となる。

【0078】

そして、ステップS54において、ドアロック機構36及びラッゲージドアロック機構39をアンロックスタンバイ状態にする。そして、図示しないが、ドアハンドルの操作の開始が検出されると、ドアやラッゲージドアをアンロック状態にする。なお、携帯機30の携帯者が車両32に乗車して、エンジンの始動禁止を解除する指示信号を出力するまでの動作は、上述の図13及び図14に示した処理と同様であるので、説明を省略する。

【0079】

(キーコード登録)

次に、本実施形態の特徴部分である、携帯機30の車両固有のキーコードを車両32のセキュリティECU35へ登録する際の動作について、図17及び図18のフローチャートを用いて説明する。

【0080】

なお、携帯機30から送信コード信号を送信する前に、セキュリティECU35をキーコード登録のモードに変更しておく。また、このとき、セキュリティECU35のRAMが記憶する、キーコードを復号化するための変換テーブル(図11と同じ)のk番目の共通鍵コード[KEY(k)]を、登録用のキーコードに変更しておく。この登録用キーコードは、上述の如く、mビットからなる変数であり、例えば、0000やffff等の変数である。

【0081】

このモード変更については、例えば、別途用意される登録専用の携帯機等からモード変更の信号を発信し、ワイヤレスレシーバ34がこれを受信してセキュリティECU35のモードを変更する。また、このモード変更がなされた場合には、セキュリティECU35はチャレンジコードを出力しないようにする。

【0082】

先ず、ステップS60は、携帯機30の押しボタンスイッチ(図示せず)によって、特定の操作がなされたか否かを判断する。ここで、特定の操作がなされた場合には、ステップS61へ処理を進め、これに該当しない場合には、スイッチ操作がなされるまで待機状態となる。この特定のスイッチがなされた場合に、携帯機30では、車両固有のキーコードを暗号化して送信するようになっているため、キーコードを容易に送信できる。

【0083】

なお、この特定のスイッチ操作とは、例えば、特定の複数のスイッチを同時に押したり、複数のスイッチを特定の順序で押したりする操作である。

【0084】

ステップS61では、図15に示すように、携帯機30のRAMに記憶される、キーコードを暗号化するための変換テーブルのk番目の共通鍵コード[KEY(k)]を、同じくRAMに記憶される登録用のキーコードに変更する。この登録用キーコードは、mビット

からなる変数であり、例えば、0 0 0 0 や f f f f 等の変数である。

【0085】

ステップS 6 2では、RAMに記憶される車両固有のキーコードを暗号化して暗号化キーコードを生成する。この暗号化キーコードの生成方法については、上述のチャレンジコードを暗号化して暗号化チャレンジコードを生成する方法と同一であり、図15に示す変換テーブルのk番目の共通鍵コードに登録用キーコードを用いた点と、図16に示すように、暗号化アルゴリズムを用いて暗号化する対象が車両固有のキーコードになる点のみ異なる。従って、暗号化キーコードの生成方法に関する説明は省略する。

【0086】

このように、本実施形態におけるキーコードの暗号化は、携帯機30から発信されたチャレンジコード信号を暗号化する際の暗号化アルゴリズムを使用するため、専用の暗号化アルゴリズムを用意する必要がなく、ソフト容量の節約や管理工数が削減できる。

【0087】

ステップS 6 3では、ステップS 6 2において暗号化された暗号化キーコード、及びRAMに記憶されるIDコードを用いて送信コードを生成する。この送信コードは、上述のように、例えば、これらの各コードにフォーマットビット（スタートビット、ストップビット、パリティビット）を付加し、さらに所定ビット数からなる乱数を加えて送信コードを構成する。そして、ステップS 6 4において、ステップS 6 3で生成した送信コードを発信する。

【0088】

続いて、ワイヤレスレシーバ34が、上述の暗号化キーコードを含む送信コードを受信してから、復元したキーコードを記憶するまでの動作について、図18のフローチャートを用いて説明する。

【0089】

まず、ステップS 7 0において、携帯機30からの送信コードをワイヤレスレシーバ34が受信したか否かを判断する。ここで、送信コードを受信した場合には、ステップS 7 1へ処理を進め、送信コードを受信していない場合には、受信するまで待機状態となる。

【0090】

ステップS 7 1では、送信コードからIDコード及び暗号化キーコードを抽出し、この抽出した暗号化キーコードを復元する。なお、暗号化キーコードの復元は、登録用キーコードが設定された変更テーブルを用いて復元する。そして、ステップS 7 2において、抽出したIDコードとセキュリティECU35のRAMに記憶されているIDコードとが一致するか否かを判断する。ここで、IDコードが一致するならば、ステップS 7 3へ処理を進め、これに該当しない場合には、ステップS 10へ処理を移行し、再び送信コードの受信待ちとなる。

【0091】

ステップS 7 3では、セキュリティECU35のRAMへ、送信コードから復元したキーコードを記憶する。あるいは、既にキーコードが記憶されている場合には、既に記憶されているキーコードを復元したキーコードに上書き記憶する。

【0092】

このように、携帯機と車両との双方向通信によって、車両の各ドアのロック機構やステアリングロック機構を制御したり、車両のエンジンの始動の許可・禁止状態を制御したりする電子キーシステムに、本実施形態の遠隔操作装置を適用することによって、固有キーコードの解読を容易にすることを防止できる。その結果、携帯機の不正な複製を防止することが可能となる。

【0093】

なお、本実施形態において説明した暗号化アルゴリズム及び復号化アルゴリズムは、排他的論理和の演算やM系列演算による暗号化に限定されるものではない。

【0094】

また、通常動作及びキーコード登録の処理において、携帯機30から発信される送信コー

10

20

30

40

50

ドに含まれるIDコードを暗号化しても良い。そして、携帯機30から暗号化されたIDコードを含む送信コードを発信し、この送信コードを受信する車両32のセキュリティECU35において暗号化されたIDコードを復元しても良い。

【図面の簡単な説明】

【図1】第1の実施形態に係わる、送信機1及び受信機2の構成を示すブロック図である。

【図2】第1の実施形態に係わる、ローリングコードを暗号化するための変更テーブルを示す図である。

【図3】第1の実施形態に係わる、暗号化アルゴリズムを示す図である。

【図4】第1の実施形態に係わる、制御対象を遠隔操作する際の送信機1の処理を示すフローチャートである。 10

【図5】第1の実施形態に係わる、制御対象を遠隔操作する際の受信機2の処理を示すフローチャートである。

【図6】第1の実施形態に係わる、キーコード登録の際に用いる、キーコードを暗号化するための変更テーブルを示す図である。

【図7】第1の実施形態に係わる、キーコードを暗号化する暗号化アルゴリズムを示す図である。

【図8】第1の実施形態に係わる、キーコードを送信する際の送信機1の処理を示すフローチャートである。

【図9】第1の実施形態に係わる、キーコードを登録する際の受信機2の処理を示すフローチャートである。 20

【図10】第2の実施形態に係わる、電子キーシステムの全体の構成を示す図である。

【図11】第2の実施形態に係わる、チャレンジコードを暗号化するための変更テーブルを示す図である。

【図12】第2の実施形態に係わる、暗号化アルゴリズムを示す図である。

【図13】第2の実施形態に係わる、携帯機30の通常動作における処理を示すフローチャートである。

【図14】第2の実施形態に係わる、車両32側の通常動作における処理を示すフローチャートである。

【図15】第2の実施形態に係わる、キーコード登録の際に用いる、キーコードを暗号化するための変更テーブルを示す図である。 30

【図16】第2の実施形態に係わる、キーコードを暗号化する暗号化アルゴリズムを示す図である。

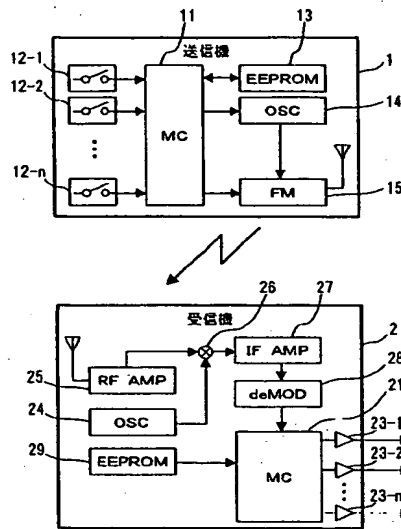
【図17】第2の実施形態に係わる、キーコード登録の際の携帯機30における処理を示すフローチャートである。

【図18】第2の実施形態に係わる、キーコード登録の際の車両32における処理を示すフローチャートである。

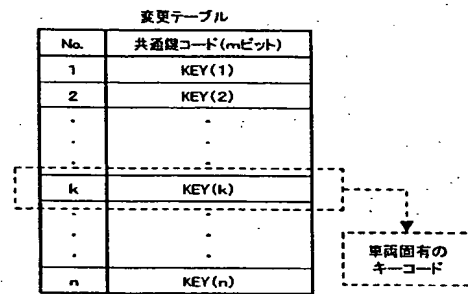
【符号の説明】

1・・・送信機、2・・・受信機、30・・・携帯機、32・・・車両、35・・・セキュリティECU

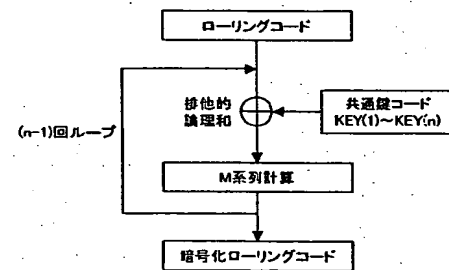
【図 1】



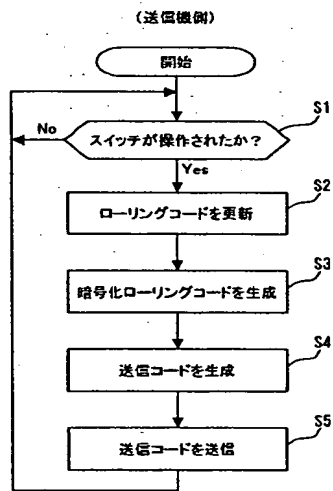
【図 2】



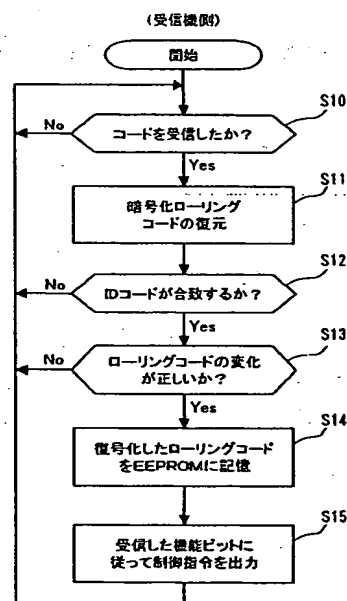
【図 3】



【図 4】



【図 5】



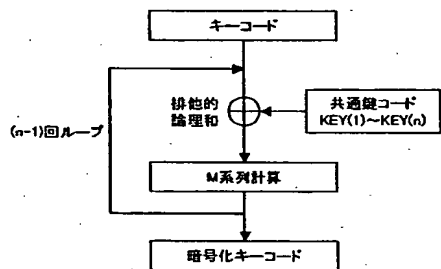
【図 6】

変更テーブル

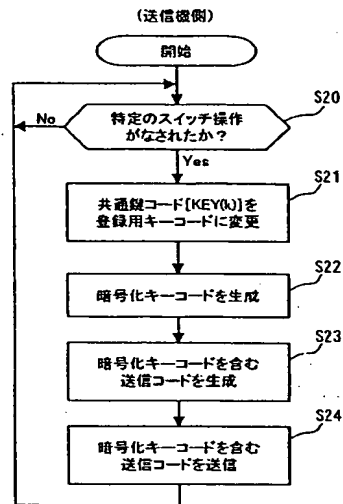
No.	共通鍵コード(mビット)
1	KEY(1)
2	KEY(2)
⋮	⋮
k	KEY(k)
⋮	⋮
n	KEY(n)

登録用キーコードに変更

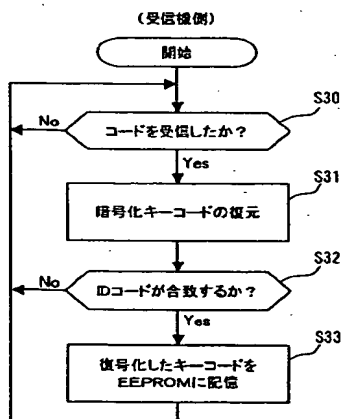
【図 7】



【図 8】



【図 9】



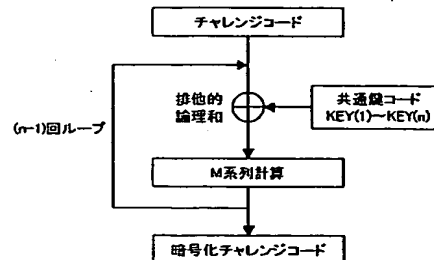
【図 11】

変更テーブル

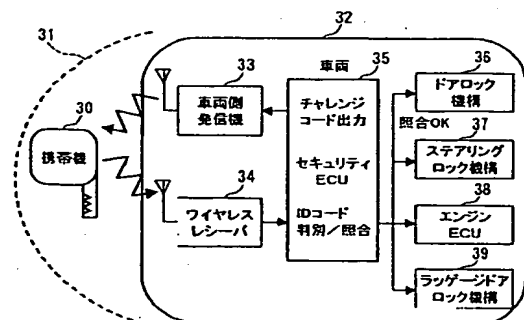
No.	共通鍵コード(mビット)
1	KEY(1)
2	KEY(2)
⋮	⋮
k	KEY(k)
⋮	⋮
n	KEY(n)

車両固有のキーコード

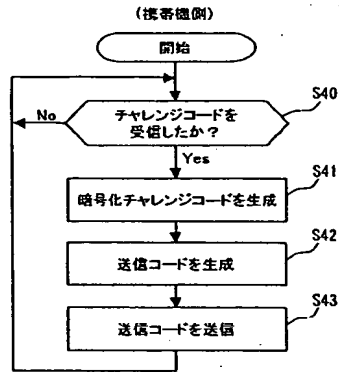
【図 12】



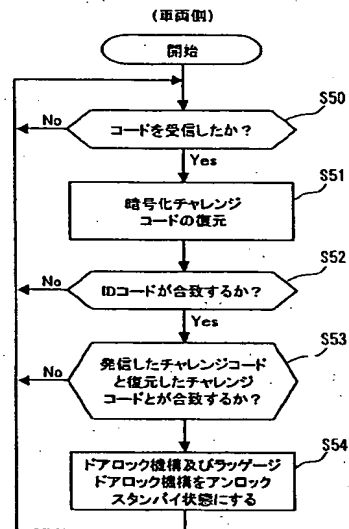
【図 10】



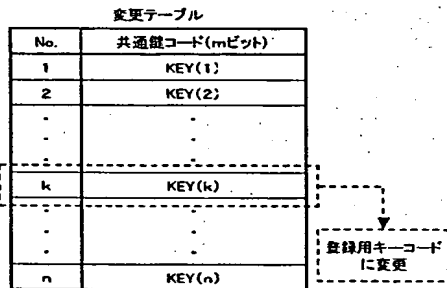
【図 1 3】



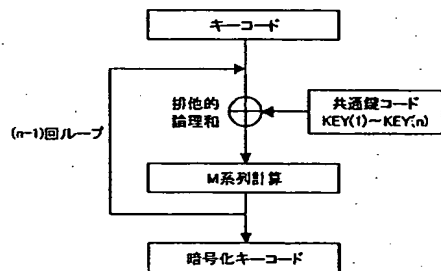
【図 1 4】



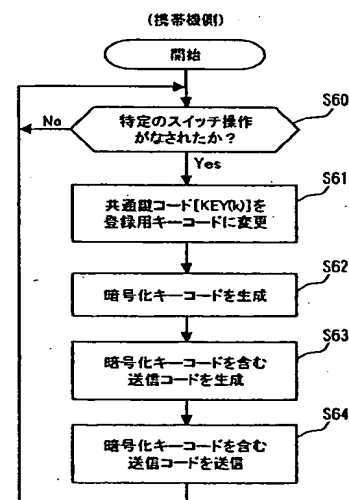
【図 1 5】



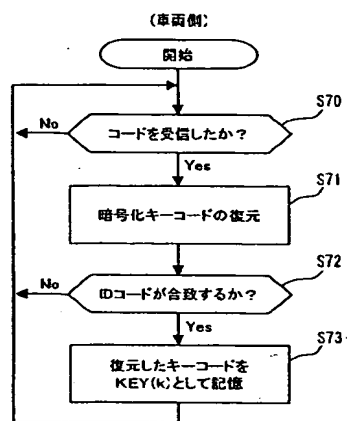
【図 1 6】



【図 1 7】



【図 18】



フロントページの続き

Fターム(参考) 5K048 AA15 BA42 BA52 DA01 DB01 DC01 EA11 EB02 FC01 HA04
HA06